

862.C2291



PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

KEIICHI IWAMURA

Application No.: 09/901,684

Filed: July 11, 2001

For: INSPECTION METHOD AND  
SYSTEM

)  
:  
) Examiner: Unassigned

)  
:  
) Group Art Unit: Unassigned

)  
:  
)  
:  
) October 16, 2001  
:  
)

2-131 #2  
**RECEIVED**  
OCT 17 2001  
Technology Center 2100

Commissioner for Patents  
Washington, D.C. 20231

CLAIM TO PRIORITY

Applicant hereby claims priority under the International Convention and all rights to which he is entitled under 35 U.S.C. § 119 based upon the following Japanese Priority Application:

2000-213204

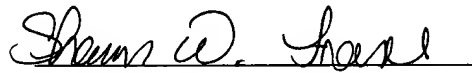
Japan

July 13, 2000.

A certified copy of the priority document is enclosed.

Applicant's undersigned attorney may be reached in our Washington, D.C. office by telephone at (202) 530-1010. All correspondence should continue to be directed to our address given below.

Respectfully submitted,

A handwritten signature in cursive script, reading "Shawn W. Fraser", is written over a horizontal line.

Attorney for Applicant  
Shawn W. Fraser  
Registration No. 45,886

FITZPATRICK, CELLA, HARPER & SCINTO  
30 Rockefeller Plaza  
New York, New York 10112-3801  
Facsimile: (212) 218-2200

SWF:eyw-

DC\_MAIN 73532 v 1



#2

(translation of the front page of the priority document of Japanese Patent Application No. 2000-213204)

PATENT OFFICE  
JAPANESE GOVERNMENT

RECEIVED  
OCT 17 2001  
Technology Center 2100

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: July 13, 2000

Application Number : Patent Application 2000-213204

Applicant(s) : Canon Kabushiki Kaisha

August 3, 2001

Commissioner,  
Patent Office

Kouzo OIKAWA

Certification Number 2001-3069436

Appln. no.: 09/901,684  
Filed: July 11, 2001  
Inv.: Keiichi Inamura  
Title: Inspection Method AND System

CFM2291 US

#2

日本国特許庁

JAPAN PATENT OFFICE

RECEIVED

OCT 17 2001

Technology Center 2100

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日

Date of Application:

2000年 7月13日

出願番号

Application Number:

特願2000-213204

出願人

Applicant(s):

キヤノン株式会社

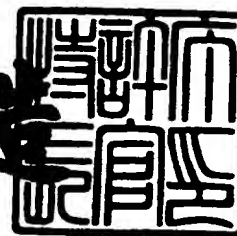


CERTIFIED COPY OF  
PRIORITY DOCUMENT

2001年 8月 3日

特許庁長官  
Commissioner,  
Japan Patent Office

及川耕造



出証番号 出証特2001-3069436

【書類名】 特許願

【整理番号】 4205040

【提出日】 平成12年 7月13日

【あて先】 特許庁長官殿

【国際特許分類】 G06G 15/00

【発明の名称】 検査方法及び検査システム

【請求項の数】 14

【発明者】

【住所又は居所】 東京都大田区下丸子3丁目30番2号 キヤノン株式会社  
社内

【氏名】 岩村 恵市

【特許出願人】

【識別番号】 000001007

【氏名又は名称】 キヤノン株式会社

【代理人】

【識別番号】 100076428

【弁理士】

【氏名又は名称】 大塚 康德

【電話番号】 03-5276-3241

【選任した代理人】

【識別番号】 100101306

【弁理士】

【氏名又は名称】 丸山 幸雄

【電話番号】 03-5276-3241

【選任した代理人】

【識別番号】 100115071

【弁理士】

【氏名又は名称】 大塚 康弘

【電話番号】 03-5276-3241

【手数料の表示】

【予納台帳番号】 003458

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0001010

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 検査方法及び検査システム

【特許請求の範囲】

【請求項 1】

ネットワークを構成する端末に格納された情報を検査する検査方法であって、  
前記端末間を移動し、前記情報に電子透かしが埋め込まれているか否かを判定  
するプログラムモジュールを利用することを特徴とする検査方法。

【請求項 2】

前記プログラムモジュールによって電子透かしが埋め込まれていると判定され  
た情報を、端末から、検査用サーバにダウンロードすることを特徴とする請求項  
1 に記載の検査方法。

【請求項 3】

前記プログラムモジュールは、前記情報に電子透かしが埋め込まれていると判  
定した場合には、該電子透かしに基づいて、前記端末のユーザが、前記情報の正  
当な利用者であるか否か判断することを特徴とする請求項 1 に記載の検査方法。

【請求項 4】

端末に格納された情報に電子透かしが埋め込まれているか否かを判定するプロ  
グラムモジュールを、ネットワークを構成する各端末間で移動させる検査用ホス  
トを含むことを特徴とする検査システム。

【請求項 5】

ネットワークを構成する各端末間を移動し、該各端末に格納された情報に、電  
子透かしが埋め込まれているか否かを判定するプログラムモジュールを格納した  
記録媒体。

【請求項 6】

ネットワーク上に電子透かし抽出技術を公開する工程と、  
前記ネットワークを構成する端末に対し、該電子透かし抽出技術の使用許諾を  
行う工程と、  
前記電子透かし抽出技術を、前記使用許諾を受けた端末を介して、他の端末に  
組み込む工程と、

前記他の端末に組み込まれた電子透かし抽出技術を用いて、前記他の端末に与えられる情報の正当性を検査する検査工程と、

を含むこと特徴とする検査方法。

【請求項 7】

前記検査工程で、情報の不正利用が検出された場合には、その旨を、前記他の端末から、著作権保護端末に、前記ネットワークを介して通知する工程を更に含むことを特徴とする請求項 6 に記載の検査方法。

【請求項 8】

ネットワーク上に電子透かし抽出技術を公開し、前記ネットワークを構成する端末に対し、該電子透かし抽出技術の使用許諾を行う電子透かし技術サーバを含むこと特徴とする検査システム。

【請求項 9】

ネットワークを介して情報の購入申し込みを受け付ける受付工程と、

前記情報の著作権を保護するために用いられている技術について、前記ネットワークを介して、提示する提示工程と、

前記情報の購入を申し込んだユーザの前記技術に対する同意を確認した場合に、前記ユーザに前記情報を提供する提供工程と、

前記技術を用いて前記情報の正当性を検査する検査工程と、

を含むことを特徴とする検査方法。

【請求項 10】

前記提示工程は、前記情報を不正利用したユーザに対して取りうる処置についても提示することを特徴とする請求項 9 に記載の検査方法。

【請求項 11】

前記提示工程は電子透かしの抽出法に関する説明、及び前記情報に埋め込んだ電子透かし情報を検査できる抽出プログラムを、ユーザに提供する工程であり、

前記提供工程は、前記同意と共に前記ユーザの識別情報を確認した場合に、前記情報に、該ユーザ識別情報を電子透かしとして埋め込んだ後に、前記ユーザにその情報を提供する工程であることを特徴とする請求項 9 に記載の検査方法。

【請求項 12】



ユーザから、ネットワークを介して、情報の購入申し込みを受付け、該申し込みに対して、前記情報の著作権を保護するために用いられている技術について、前記ネットワークを介して、前記ユーザに提示し、前記情報の販売の条件として、前記ユーザに対して、前記技術に対する同意を求める情報販売サーバを含むことを特徴とする検査システム。

【請求項 1 3】

暗号化された情報であって、かつ、記憶媒体識別情報が電子透かしとして埋め込まれた情報を格納した記憶媒体を提供する記憶媒体提供工程と、

前記ユーザに対し、前記記憶媒体識別情報及びユーザ識別情報の提示を求める提示要求工程と、

前記提示と引き替えに、前記暗号化された情報の復号プログラムを前記ユーザに提供する提供工程と、

前記情報に電子透かしとして埋め込まれた記憶媒体識別情報から導きだされた前記ユーザ識別情報と、前記情報が格納された端末のユーザ情報と、を比較することにより、前記情報の正当性を検査する検査工程と、

を有することを特徴とする検査方法。

【請求項 1 4】

暗号化され、かつ、記憶媒体識別情報が電子透かしとして埋め込まれた情報を、記憶媒体に格納し、販売する検査システムであって、

前記ユーザから、前記記憶媒体識別情報及びユーザ識別情報の提示があった場合に、前記暗号化された情報の復号ソフトを前記ユーザに提供し、

前記記憶媒体識別情報とユーザ識別情報とを対応させて管理し、

前記情報に電子透かしとして埋め込まれた記憶媒体識別情報から導きだされた前記ユーザ識別情報と、前記情報が格納された端末のユーザ情報と、を比較することにより、前記情報の正当性を検査することを特徴とする検査システム。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、動画像データ、静止画像データ、音声データ、コンピュータデータ

、コンピュータプログラム等の情報を検査する検査方法及び検査システムに関するものである。

【0002】

【従来の技術】

近年のコンピュータ及びネットワークの発達は著しく、文字データ、画像データ、音声データ等、多種の情報がコンピュータ内、ネットワーク内で扱われるようになってきている。よって、デジタルの静止画像や動画や音楽などのいわゆるデジタルコンテンツをネットワーク上で売買するコンテンツビジネスが盛んに行われるようになってきている。

【0003】

コンテンツビジネスの対象となる情報はデジタルデータであるために、複製を容易に作成できる環境にある。こうしたデータの著作権を保護する方法としては、例えば、データ中に、著作権情報や利用者情報を、電子透かしとして埋め込む方法がある。ここで、電子透かしとは、著作権保護のために、著作物としてのデータに対して加えられるいかなる処理をも含む概念であり、例えば、そのデータの内容に影響を与えることなく埋め込まれた、利用者識別情報である。

【0004】

この電子透かしをデータから抽出することにより、著作者や利用者等の識別情報を得ることができる。従って、例えば、ある利用者Aを示す電子透かしが埋め込まれた画像データを、利用者Bが利用していることが判明した場合には、利用者A及び／又は利用者Bが不正コピーや不正利用を行ったことになる。

【0005】

電子透かし技術の例としては空間領域に埋め込む方式と周波数領域に埋め込む方法の二つに大きく分類でき、種々の方法が知られている。

【0006】

空間領域に埋め込む方式の例としては、パッチワークによるものとしてIBMの方式(W.Bender,D.Gruhl,N.Morimoto,Techniques for Data Hiding,"Proceedings of the SPIE,San Jose CA,USA,February 1995)やG.B.Rhoads,W.Linn:"Steganographymethods employing embedded", "USP Patent Number5,636,292などが挙げ

られる。

【0007】

周波数領域に埋め込む方式の例としては、離散コサイン変換を利用するものとしてNTTの方式（中村，小川，高嶋，” デジタル画像の著作権保護のための周波数領域における電子透かし方式”， SCIS' 97-26A， 1997年1月）の他に、離散フーリエ変換を利用するものとして防衛大の方式（大西，岡，松井，” PN系列による画像への透かし署名法”， SCIS' 9726B， 1997年1月）や離散ウェーブレット変換を利用するものとして三菱，九大の方式（石塚，坂井，櫻井，” ウェーブレット変換を用いた電子透かし技術の安全性と信頼性に関する実験的考察”， SCIS' 97-26D， 1997年1月）及び松下の方式（” ウェーブレット変換に基づくデジタル・ウォーターマークー画像圧縮，変換処理に対するロバスト性について”， 井上，宮崎，山本，桂， SCIS' 98-3. 2. A， 1998年1月）などが挙げられる。

【0008】

また、電子透かし技術を用いて不正コピーを検査するシステムも、Digimarc社のUSP5862260やNTTの持開平11-39263，特開平11-66009に提案されている。

【0009】

これらの電子透かし技術は、商用として用いられる際には、アルゴリズムを完全に秘密にする事を前提として利用される（このような電子透かし埋め込みシステムを秘密鍵方式と称す）。アルゴリズムや情報の埋め込み場所などに関する情報が秘密であることを根拠にして、電子透かし技術の安全性が図られる。その秘密情報が漏洩した場合、コンテンツの不正配布を企むユーザは、入手した情報を解析して埋め込まれた電子透かしを特定し、その部分を変形することにより不正利用の証拠となる情報（著作権情報やユーザ情報など）を破壊し、罪を免れることができる。

【0010】

【発明が解決しようとする課題】

しかしながら、従来の著作権保護技術では、非効率的で、不確実であるという

問題があった。例えば、秘密鍵方式の電子透かし埋め込みシステムにおいては、そのアルゴリズムの漏洩を防止するために様々な対策がとられており、結果として、検査負担が膨大であるという問題点、標準化が困難であるという問題点、そして、不正利用の証明が困難であるという問題点が存在している。

【0011】

本発明は、これらの問題点を解決するためになされたものであり、その目的とするところは、効率的に且つ確実に著作権を保護することのできる検査方法及び検査システムを提供することにある。

【0012】

【課題を解決するための手段】

上記目的を達成するため、本発明に係る方法は、  
ネットワークを構成する端末に格納された情報を検査する検査方法であって、  
前記端末間を移動し、前記情報に電子透かしが埋め込まれているか否かを判定するプログラムモジュールを利用することを特徴とする。

【0013】

前記プログラムモジュールによって電子透かしが埋め込まれていると判定された情報を、端末から、検査用サーバにダウンロードすることを特徴とする。

【0014】

前記プログラムモジュールは、前記情報に電子透かしが埋め込まれていると判定した場合には、該電子透かしに基づいて、前記端末のユーザが、前記情報の正当な利用者であるか否かを判断することを特徴とする。

【0015】

端末に格納された情報に電子透かしが埋め込まれているか否かを判定するプログラムモジュールを、ネットワークを構成する各端末間で移動させる検査用ホストを含むことを特徴とする。

【0016】

上記目的を達成するため、本発明に係る記憶媒体は、  
ネットワークを構成する各端末間を移動し、該各端末に格納された情報に、電子透かしが埋め込まれているか否かを判定するプログラムモジュールを格納した

記録媒体。

【 0 0 1 7 】

ネットワーク上に電子透かし抽出技術を公開する工程と、

前記ネットワークを構成する端末に対し、該電子透かし抽出技術の使用許諾を行う工程と、

前記電子透かし抽出技術を、前記使用許諾を受けた端末を介して、他の端末に組み込む工程と、

前記他の端末に組み込まれた電子透かし抽出技術を用いて、前記他の端末に与えられる情報の正当性を検査する検査工程と、

を含むこと特徴とする。

【 0 0 1 8 】

前記検査工程で、情報の不正利用が検出された場合には、その旨を、前記他の端末から、著作権保護端末に、前記ネットワークを介して通知する工程を更に含むことを特徴とする。

【 0 0 1 9 】

ネットワーク上に電子透かし抽出技術を公開し、前記ネットワークを構成する端末に対し、該電子透かし抽出技術の使用許諾を行う電子透かし技術サーバを含むこと特徴とする。

【 0 0 2 0 】

ネットワークを介して情報の購入申し込みを受け付ける受付工程と、

前記情報の著作権を保護するために用いられている技術について、前記ネットワークを介して、提示する提示工程と、

前記情報の購入を申し込んだユーザの前記技術に対する同意を確認した場合に、前記ユーザに前記情報を提供する提供工程と、

前記技術を用いて前記情報の正当性を検査する検査工程と、

を含むことを特徴とする。

【 0 0 2 1 】

前記提示工程は、前記情報を不正利用したユーザに対して取りうる処置についても提示することを特徴とする。

【 0 0 2 2 】

前記提示工程は電子透かしの抽出法に関する説明、及び前記情報に埋め込んだ電子透かし情報を検査できる抽出プログラムを、ユーザに提供する工程であり、

前記提供工程は、前記同意と共に前記ユーザの識別情報を確認した場合に、前記情報に、該ユーザ識別情報を電子透かしとして埋め込んだ後に、前記ユーザにその情報を提供する工程であることを特徴とする。

【 0 0 2 3 】

ユーザから、ネットワークを介して、情報の購入申し込みを受付け、該申し込みに対して、前記情報の著作権を保護するために用いられている技術について、前記ネットワークを介して、前記ユーザに提示し、前記情報の販売の条件として、前記ユーザに対して、前記技術に対する同意を求める情報販売サーバを含むことを特徴とする。

【 0 0 2 4 】

暗号化された情報であって、かつ、記憶媒体識別情報が電子透かしとして埋め込まれた情報を格納した記憶媒体を提供する記憶媒体提供工程と、

前記ユーザに対し、前記記憶媒体識別情報及びユーザ識別情報の提示を求める提示要求工程と、

前記提示と引き替えに、前記暗号化された情報の復号プログラムを前記ユーザに提供する提供工程と、

前記情報に電子透かしとして埋め込まれた記憶媒体識別情報から導きだされた前記ユーザ識別情報と、前記情報が格納された端末のユーザ情報と、を比較することにより、前記情報の正当性を検査する検査工程と、

を有することを特徴とする。

【 0 0 2 5 】

暗号化され、かつ、記憶媒体識別情報が電子透かしとして埋め込まれた情報を、記憶媒体に格納し、販売する検査システムであって、

前記ユーザから、前記記憶媒体識別情報及びユーザ識別情報の提示があった場合に、前記暗号化された情報の復号ソフトを前記ユーザに提供し、

前記記憶媒体識別情報とユーザ識別情報とを対応させて管理し、

前記情報に電子透かしとして埋め込まれた記憶媒体識別情報から導きだされた前記ユーザ識別情報と、前記情報が格納された端末のユーザ情報と、を比較することにより、前記情報の正当性を検査することを特徴とする。

【 0 0 2 6 】

【発明の実施の形態】

以下に、図面を参照して、この発明の好適な実施の形態を例示的に詳しく説明する。ただし、この実施の形態に記載されている構成要素の相対配置、数式、数値等は、特に特定の記載がない限りは、この発明の範囲をそれらのみに限定する趣旨のものではない。

【 0 0 2 7 】

(第 1 の実施の形態)

本発明に係る情報処理システムの第 1 の実施の形態として、ディジタルコンテンツの不正利用検査システムについて説明する。

【 0 0 2 8 】

このシステムは、電子透かしの抽出機能をもつエージェントをネットワーク上で移動させ（モビリティ）、ネットワークを構成する各端末において電子透かし抽出を行わせて、その結果に基づいてコンテンツを送信するかどうか判断し（インテリジェンス）、その結果を検査局に通信させる（コミュニケーション）ことにより、ディジタルコンテンツの不正利用検査するものである。

【 0 0 2 9 】

USP 5 8 6 2 2 6 0 や特開平 1 1 - 3 9 2 6 3, 特開平 1 1 - 6 6 0 0 9 に開示された検査システムは、電子透かしに関する情報の機密性を保つため、ユーザ側の端末ではなく情報の守秘が行われる検査局でその抽出処理を行うことが前提になっている。つまり、ネットワーク上でアクセスできるユーザ端末のコンテンツをまず検査局にダウンロードし、検査局で電子透かしの抽出処理を行い、コンテンツが不正に利用されていないかを検査する。

【 0 0 3 0 】

従って、USP 5 8 6 2 2 6 8 や特開平 1 1 - 3 9 2 6 3, 特開平 1 1 - 6 6 0 0 9 に開示された従来の検査システムでは、完全な検査を実行しようとする

アクセス可能なコンテンツ全てを検査局にダウンロードする必要がある、そのために必要な通信量、コストは膨大なものになるという問題点があった。また、全てのコンテンツが1つまたは少数の検査局に集中するために検査局の負荷も膨大であるという問題点があった。

#### 【0031】

これに対して、本実施の形態では、ロボットエージェントをネットワーク上に走らせ、各端末において、その端末が有するコンテンツ内に電子透かしが埋め込まれているか否かを判断し、電子透かしが埋め込まれているもののみを検査局にダウンロードする。そうすれば、ダウンロードに必要な通信量を大幅に削減することができ、検査局への情報の集中も緩和できる。

#### 【0032】

ここで、エージェントについて簡単に説明する。エージェントとは仮想的な主体によって人間の情報処理を代行させる技術の総称である。エージェントがもつ能力を分類すると、大きく3つに分類することができる。「インテリジェンス」、「コミュニケーション」、及び「モビリティ」である。

#### 【0033】

インテリジェンスは、個々のエージェントの問題解決に関する能力である。エージェントがさまざまな状況で自らの行動を決定するためには、ある程度の推論やプランニングを余儀なくされる。インテリジェンスの低いエージェントは状況の変化に対応した処理ができずに、ユーザや他のシステムからの入力をトリガとした即応的な行為しかできなくなる。また、常に複雑な推論やプランニングを行った結果として行動を決定する熟考型のエージェントが、自分が行うべき行為の機会を逸してしまうこともありえる。つまり、インテリジェンスには、推論したりプランニングするだけでなく、即応性とのバランスをとる能力も含まれる。

#### 【0034】

コミュニケーションは、エージェントが他のエージェントと情報を交換したり、タスクの遂行を要求したりする能力である。複数のエージェントが協力するマルチエージェントシステムにおいて必須の技術となる。また、ユーザの要求をどのように知り、エージェントの作業状況をどのようにユーザに示すかも、エー



エントのコミュニケーションの問題である。これは、エージェントシステムのユーザインタフェースを考える上で非常に重要である。

【 0 0 3 5 】

モビリティは、エージェントが自分の活動する計算機環境を移り変わる能力である。必要な計算資源を求めてネットワーク上を移動するモバイルエージェントにとって本質となる技術である。もし、必要な資源とそれを管理するエージェントとコミュニケーションを行うことによって問題を解決できる場合もあるが、自分がその資源のあるマシンに移動して情報処理してしまった方が都合がよい場合もある。モビリティとは、そのような行動の自由度をエージェントにもたらしものである。

【 0 0 3 6 】

以上、エージェントについて概略を説明したが、これらの詳細は、「特集 最新エージェントテクノロジー」(bit February 1999/Vol.31, No.2, pp.2-34)などに記載されている。

【 0 0 3 7 】

次に、本実施の形態としての不正利用検査システムの概要を図 1 に示す。

【 0 0 3 8 】

1 0 1 はエージェント 1 0 2 を作成してデジタルコンテンツの不正利用を監視する検査局であり、ネットワーク 1 0 3 に接続されている。1 0 4 ~ 1 0 5 はネットワーク 1 0 3 に接続されている各ユーザの端末である。ネットワーク 1 0 3 には、インターネット等であればよい。

【 0 0 3 9 】

エージェント 1 0 2 は、図 2 のような内部構成をしており、電子透かし抽出モジュール 3 0 1 と、他のエージェントや端末、検査局と通信を行うコミュニケーションモジュール 3 0 3 と、検査局やユーザ端末間を移動するモビリティモジュール 3 0 4 とが、インテリジェンスモジュール 3 0 2 によって制御される。

【 0 0 4 0 】

本システムにおける処理の流れについて、図 3 のフローチャートを用いて説明する。

## 【 0 0 4 1 】

検査局 1 0 1 は、エージェント 1 0 2 を作成し（ステップ S 2 0 1）、ネットワーク 1 0 3 を用いて移動させる（ステップ S 2 0 2）。エージェント 1 0 2 はユーザ 1 0 4 の端末に移動し、その端末においてアクセスできるデジタルコンテンツを電子透かし抽出モジュール 3 0 1 を用いて検査し（ステップ S 2 0 3）、その検査結果やユーザ名などをコミュニケーションモジュール 3 0 3 を用いて検査局 1 0 1 に送信する（ステップ S 2 0 4）。ここで、検査したデジタルコンテンツから電子透かしが抽出された場合（ステップ S 2 0 5）、そのコンテンツを検査局に送信する（ステップ S 2 0 6）。検査したデジタルコンテンツから電子透かしが抽出されなかった場合（ステップ S 2 0 5）、不正利用ではないとしてコンテンツの送信は行わない。すべてのコンテンツを検査した後、エージェント 1 0 2 は次のユーザ端末 1 0 5 に移動して（ステップ S 2 0 7）、その端末でアクセスできるデジタルコンテンツに対して 2 0 3 以降の動作を繰り返す。調査するユーザ端末数や終了時間などの、エージェントに設定された終了条件がくれば（ステップ S 2 0 7）、検査局 1 0 1 に移動し処理を終了する。

## 【 0 0 4 2 】

上述したように、本実施の形態によれば、デジタルコンテンツを最初に検査局に送信せず、電子透かしを検査して、電子透かしが抽出されたコンテンツのみを送信するために通信量やコストが低い。検査局はそのコンテンツを利用しているユーザが正当なユーザかどうかを電子透かし情報を用いて検査すればよいために負荷が少ない。なお、エージェントのインテリジェンスを高くして、ステップ S 2 0 5 において抽出された電子透かし情報とそのユーザ端末を解析して、正当なユーザである場合はコンテンツを送信せず、正当なユーザでない場合のみコンテンツを送信するようにすれば、通信量やコストはさらに低く、検査局の負荷も少なくなり、検査局は不正利用のユーザに警告を行い不正利用を止めさせるなどの処理に専念できる。

## 【 0 0 4 3 】

また、エージェントによって判定不可能なコンテンツが存在する場合には、そのコンテンツも検査局に送信するようにすれば不確実性を排除できる。

## 【 0 0 4 4 】

一方、電子透かしのアルゴリズム及び電子透かし情報の埋め込み位置などを公開できる電子透かし手法が特開平 1 1 - 2 8 9 2 5 5 に示されている。これによれば、デジタルコンテンツ全体を誤り訂正符号化することによって、公開された位置にある埋め込み情報が破壊されてもコンテンツ全体から埋め込み情報の復元が行える。電子透かしアルゴリズムに依存せず誤り訂正を行うので、電子透かしアルゴリズムを公開することもできる。このようにアルゴリズムや埋め込み位置が公開できる電子透かし手法を、ここでは公開鍵電子透かし方式と呼ぶ。

## 【 0 0 4 5 】

アルゴリズムや電子透かしの埋め込み位置を公開できるこの方式を利用すれば、エージェント内に組み込まれた電子透かし抽出モジュールをユーザ端末で解析されたり、解析された電子透かし位置を破壊されても、情報を復元できるので安全である。

## 【 0 0 4 6 】

## (第 2 の実施の形態)

第 1 の実施の形態では 1 つの検査局と 1 つのエージェントで検査を行う場合を説明した。本実施の形態では 1 つまたは複数の検査局と複数のエージェントで検査を行うシステムを説明する。

## 【 0 0 4 7 】

図 4 に 1 つの検査局と複数のエージェントで検査を行うシステムを示す。

## 【 0 0 4 8 】

検査局 4 0 1 は複数のエージェント 4 0 2, 4 0 3 を作成してネットワーク 4 0 4 を介して各ユーザの端末 4 0 5, 4 0 6 のデジタルコンテンツの検査を行う。システムを構成する各要素は第 1 の実施の形態とほぼ同様であるが、違いは以下の点である。

## 【 0 0 4 9 】

検査局 4 0 1 は各エージェントが同じユーザ端末を検査しないように、各エージェントの分担をインテリジェンスモジュールに組み込み制御させる。たとえば、エージェント 4 0 2 は URL の組織の識別子が、c o の端末を担当し、エー

ェント 4 0 3 が、n e の端末を担当すれば、組織毎の分担が行える。これによって、1 つの検査局で複数の検査が同時に行えることになり飛躍的な検査の効率化が行える。

#### 【 0 0 5 0 】

図 5 に複数の検査局と複数のエージェントで検査を行うシステムを示す。

#### 【 0 0 5 1 】

5 0 1, 5 0 2 は複数の検査局であり、各検査局は複数のエージェント 5 0 3 ~ 5 0 6 を作成して 5 0 7 のネットワークを介して 5 0 8, 5 0 9 の各ユーザの端末のデジタルコンテンツの検査を行う。このシステムは図 4 のシステムを複数の検査局が独立または共同して動作させたものと考えることができる。これは国ごとに著作権保護の基準が異なるために 1 つの検査局で処理が行えない場合などに有効であると考えられる。また、地域ごとに検査局を運営する場合なども考えられる。

#### 【 0 0 5 2 】

(第 3 の実施の形態)

図 6 乃至図 1 0 を用いて本発明の第 3 の実施の形態について説明する。

#### 【 0 0 5 3 】

本実施の形態は、公開鍵方式の電子透かし技術を用いることにより、特定の管理局が無くても、多くの端末が電子透かし手段を実装できるシステムに係るものである。

#### 【 0 0 5 4 】

図 6 は、本実施の形態としての情報処理システムの概略構成図である。

#### 【 0 0 5 5 】

6 0 1 はインターネットなどのネットワークであり、6 0 2 はネットワーク 6 0 1 に接続され電子透かし埋め込み方法を公開する標準局の端末であり、6 0 3 はネットワーク 6 0 1 に接続され電子透かし手法を実装する企業・組織・個人（以後まとめて企業と表す）の端末であり、6 0 4 はネットワーク 6 0 1 に接続され企業 6 0 3 によって電子透かし手法が実装されユーザに購入された装置であり、6 0 5 はネットワーク 6 0 1 に接続され外部からソフトウェアなどをインストール

ール可能なユーザ端末であり、606はネットワーク601に接続されデジタルコンテンツの不正利用を監視する監視局の端末である。

【0056】

図7は、この情報処理システムの処理の流れを示すフローチャートである。

【0057】

標準局602は定められた電子透かし手法のアルゴリズムや利用条件などの情報をホームページ等を用いてネットワーク601上に公開する（ステップS701）。ここでは、そのホームページ等に電子透かし使用の許諾手続きなどが示されているものとする。また、詳細な情報をホームページ等からダウンロードできるようになっていてもよい。その場合、公開される情報は電子透かしの装置への実装に必要な全ての情報が含まれていてもよいし、許諾審査後に全ての情報が分かるように分割された一部の情報でもよい。ただし、分割情報である場合は許諾後に残りの情報が送信される。

【0058】

公開された電子透かしの埋め込み方法を実施したいと考える企業・組織・個人603は、ネットワーク601を介して、又は標準局602が指定する手続きに従って、標準局602にその使用許諾を申請する（ステップS702）。

【0059】

ネットワークを介した申請の場合には、標準局602から申請書一式がダウンロードできるようになっており、企業603はそれをダウンロードして指定の記述を満たした申請書として標準局602にネットワークを介して送り返す。或いは、標準局602のホームページ上に、申請書用のファイルが公開され、それをネットワークを通じて企業603が入力していく形式でもよい。次に、企業603が標準局602の許諾条件を満たすかどうか審査される（ステップS703）。この審査は標準局602が定めた機械的なフローチャート等によって行われてもよい。使用が許諾されないとき終了する。

【0060】

使用が許諾された場合、標準局602は企業603からの申請処理時や許諾処理時に得られた企業情報をデータベースなどに保存し管理する（ステップS70

4)。企業603は許諾された電子透かし抽出プログラムを装置604に格納する（ステップS705）。

【0061】

ただし、ステップS701において電子透かし手法の実装に関する全ての情報が公開されている場合、ステップS702～704の申請／許諾／管理の工程は省略することができる。また、602～606で示された各端末及び装置は一般的なコンピュータによって実現できる。また、装置604はプリンタやスキャナなどの専用装置でもよい。

【0062】

本実施の形態によれば、電子透かし手法を、守秘義務を課することなく利用許諾できるシステムが構築できる。また、このシステムによれば、企業が製作する多くの装置に同じ電子透かし手法が適用されるので、標準的な電子透かし手法を有するシステムが構築できる。

【0063】

図8に、端末のハードウェア構成例を示す。

【0064】

ホストコンピュータ801は例えば一般に普及しているパソコンであり、スキャナ814から読み取られた画像を入力し、編集・保管することが可能である。更に、ここで得られた画像をプリンタ815から印刷させることが可能である。また、ユーザーからの各種マニュアル指示等は、マウス812、キーボード813からの入力により行われる。

【0065】

ホストコンピュータ801の内部では、バス816により後述する各ブロックが接続され、種々のデータの受け渡しが可能である。

【0066】

803は、内部の各ブロックの動作を制御、或いは内部に記憶されたプログラムを実行することのできるCPUである。

【0067】

804は、印刷されることが認められていない特定画像を記憶したり、あらか

じめ必要な画像処理プログラム等を記憶しておくROMである。

【0068】

805は、CPUにて処理を行うために一時的にプログラムや処理対象の画像データを格納しておくRAMである。

【0069】

806は、RAM等に転送されるプログラムや画像データをあらかじめ格納したり、処理後の画像データを保存することのできるハードディスク（HD）である。

【0070】

807は、原稿或いはフィルム等をCCDにて読み取り、画像データを生成するスキャナと接続し、スキャナで得られた画像データを入力することのできるスキャナインターフェイス（I/F）である。

【0071】

808は、外部記憶媒体の一つであるCD（CD-R）に記憶されたデータを読み込み或いは書き出すことのできるCDドライブである。

【0072】

809は、808と同様にFDからの読み込み、FDへの書き出しができるFDドライブである。810も、808と同様にDVDからの読み込み、DVDへの書き出しができるDVDドライブである。尚、CD、FD、DVD等に画像編集用のプログラム、或いはプリンタドライバが記憶されている場合には、これらプログラムをHD806上にインストールし、必要に応じてRAM805に転送されるようになっている。

【0073】

811は、マウス812或いはキーボード813からの入力指示を受け付けるためにこれらと接続されるインターフェイス（I/F）である。

【0074】

818はモデムでありインターフェース819（I/F）を介して外部のネットワークを接続されている。

【0075】

次に、ここで販売された装置の動作について、図9のフローチャートを用いて説明する。

【0076】

出荷された装置604はユーザに購入されネットワーク601に接続され起動される（ステップS901）。起動された装置604は実装された電子透かし抽出手段によって、入力されるコンテンツを自動的に検査する（ステップS902）。ここで入力されるコンテンツはデジタルコンテンツでもよいし、装置がスキャナなどの場合は印刷されたコンテンツでもよい。装置604は抽出された電子透かし情報を解析して、そのコンテンツが不正利用されていないか判定する（ステップS903）。不正利用の場合、装置604はネットワーク601を介して監視局606に通報する（ステップS904）。不正利用と判定された場合、404の通報だけでなく装置の処理をとめるなどの処理を行ってもよい。また、電子透かし情報に監視局606のURL等が含まれている場合、自動的に監視局にリンクするなどの処理も考えられる。不正利用でない場合、通報は行われず、他のコンテンツを検査する。

【0077】

なお、装置604に電子透かし抽出手法が実装されていない場合でも、次のようにして不正利用検査システムを構築することができる。

【0078】

ユーザ端末605は標準局602から公開されている電子透かし抽出ソフトをダウンロードする（ステップS1001）。ここで、電子透かし抽出ソフトは標準局が、公開している電子透かしアルゴリズムに基づいて作成してもよいし、企業が自社開発したものを標準局の許可を得て公開したものでもよい。ユーザ端末605はダウンロードした電子透かし抽出ソフトによって任意のコンテンツを検査する（ステップS1002）。ここで検査されるコンテンツはユーザ端末605がネットワーク601を利用してアクセスできるコンテンツを対象とする。また、ユーザ端末がスキャナなどを有する場合、印刷されたコンテンツでもよい。ユーザ端末605は抽出された電子透かし情報を解析して、そのコンテンツが不正利用されていないか判定する（ステップS1003）。不正利用の場合、ユー



ザ端末 6 0 5 はネットワーク 6 0 1 を介して監視局 6 0 6 に通報する（ステップ S 1 0 0 4）。不正利用でない場合、通報は行われない。電子透かし情報に監視局 6 0 6 の URL 等が含まれている場合、自動的に監視局にリンクするなどの処理も考えられる。

【0079】

なお、ここでは公開鍵方式の電子透かしを用いたシステムについて説明したが、アルゴリズムあるいは埋め込み位置を秘密にすることを前提とした、秘密鍵方式の電子透かし技術であっても、電子透かしを解析することが困難であれば、同様の効果をもつシステムを構築できる。よって、本実施の形態は公開鍵電子透かし、秘密鍵電子透かしを問わず、ユーザ端末側でデジタルコンテンツの配布を行うシステムすべてを含む。

【0080】

本実施の形態によれば、アルゴリズムや電子透かしの埋め込み位置を公開できる電子透かし手法を用いることにより、ネットワークを用いて利用申請／許諾が行えるシステムが構築できる。このシステムによって多くの装置に同じ電子透かし手法が実装されるので、標準的な電子透かし手法を有するシステムが構築できる。また、標準的な電子透かし手法を利用して、効率的に不正検査が行えるシステムも構築できる。

【0081】

（第 4 の実施の形態）

図 1 1 及び図 1 2 を用いて本発明の第 4 の実施の形態について説明する。

【0082】

本実施の形態は、公開鍵方式の電子透かし技術を用いることにより、ネットワーク上で電子透かし技術の原理やアルゴリズムを説明し、ユーザの確認をネットワークを介してとることにより、不正利用をしたと指摘されたユーザが否認できないようなシステムに係るものである。

【0083】

図 1 1 は、本実施の形態としてのシステムの概略構成図である。

【0084】

1101はインターネットなどのネットワークであり、1102はネットワーク1101に接続されたPCなどのユーザ端末であり、1103はネットワーク1103に接続されたユーザからの注文に応じてデジタルコンテンツの販売や電子透かし埋め込みを行う販売局であり、1104はユーザ1102によって購入されそのユーザのIDなどが電子透かしとして埋め込まれているデジタルコンテンツであり、1105はデジタルコンテンツ1104の利用条件や電子透かし手法などの説明及び電子透かし情報を抽出するためのソフトウェアであり、1106はソフトウェア1105によって確認された情報（コンテンツの利用条件や不正利用した場合の処置や電子透かしの抽出法など）に対するユーザの同意書ファイルである。

## 【0085】

次に、本システムの動作を図12のフローチャートを用いて説明する。

## 【0086】

ユーザ1102はネットワーク1101を介して販売局103にデジタルコンテンツの購入を申し込む（ステップS1201）。販売局103は、コンテンツの利用条件や不正利用した場合の処置及び電子透かしの抽出法に関する説明、及び埋め込んだ電子透かし情報を検査できる抽出ソフト1105を、ユーザ102に送付する（ステップS1202）。電子透かし抽出ソフトにはサンプルコンテンツがあり練習できるようになっていてもよい。次に、ユーザは受け取った説明／抽出ソフト1105を用いて説明を理解し同意書1106を作成し販売局1103に送信する（ステップS1203）。この同意書作成及び送付は説明／抽出ソフト1105によってユーザからのいくつかの入力以外は自動的に行われるようになっていてもよい。販売局1103は同意書1106を確認して保存する（ステップS1204）。さらに、販売局1103はユーザ1102が購入を申請したコンテンツ1104にユーザIDなどの電子透かしを埋め込みユーザ1102に送信する（ステップS1205）。ユーザ1102は説明／抽出ソフト1105を用いて送られてきたコンテンツ1104を検査し、電子透かし情報を確認する。

## 【0087】

ユーザ 1 1 0 2 が説明／抽出ソフト 1 1 0 5 を用いてコンテンツ 1 1 0 4 の電子透かしを検査できなかったり、不当な内容の電子透かしが抽出された場合には、販売局 1 1 0 3 はコンテンツ販売以後の一定期間を解約可能期間としてコンテンツ 1 1 0 4 と抽出ソフト 1 1 0 5 を送り返してもらうようにすれば、その期間内にユーザによる電子透かしの破壊または改ざんが成功しない限り、ユーザが虚偽の苦情を言うことはできないので問題はなくなる。

## 【 0 0 8 8 】

また、申込書や同意書には公開鍵証明書に基づいたユーザ 1 1 0 2 によるデジタル署名などが行われていることが望ましい。公開鍵証明書とは認証局という信用のおける第三者機関から発行される識別名（個人を特定するための名前）とそのユーザの公開鍵に対して認証局の署名が施されたデータである。認証局の署名を施すことにより内容の改ざんを防止するとともに、証明書を受け取ったユーザは認証局を信用することにより証明書内の公開鍵が申請したユーザのものであることを検証することができる。つまり、公開鍵と現実世界のユーザ（またはサーバなど）を確実にバインドする仕組みである。

## 【 0 0 8 9 】

また、同意書の作成及び確認保存のステップは省略することもできる。この場合、ユーザの同意書はないが説明／抽出ソフトを用いて電子透かしを含む著作権保護に関する説明が行われることは公然の事実であるので、従来の電子透かし手法など著作権保護に関する説明が行われないシステムに比べ不正利用が発覚したときのユーザ、及び第 3 者に対する正当性は比較にならないことは明らかである。

## 【 0 0 9 0 】

（第 5 の実施の形態）

次に、図 1 3 乃至図 1 5 を用いて本発明の第 5 の実施の形態について説明する。

## 【 0 0 9 1 】

第 4 の実施の形態はコンテンツのネットワーク販売システムに係るものであるのに対し、本実施の形態は、CD-ROM などによるコンテンツ販売システムに

係る。

【 0 0 9 2 】

図 1 3 は、本実施の形態としてのシステムの概略構成図である。

【 0 0 9 3 】

1 3 0 1 はインターネットなどのネットワークであり、1 3 0 2 はユーザ端末であり、1 3 0 3 はユーザからの注文に応じてデジタルコンテンツ 1 3 0 4 の復号鍵を送信しユーザデータを管理する販売局であり、1 3 0 4 は CD-ROM 1 3 0 7 に入っておりその CD-ROM 番号やコンテンツ ID などが電子透かしとして埋め込まれかつ暗号化されているデジタルコンテンツであり、1 3 0 5 はコンテンツ 1 3 0 4 の利用条件や暗号の復号法や電子透かし手法の説明及び電子透かし情報を抽出するためのソフトウェアであり、1 3 0 6 は 1 3 0 5 のソフトウェアによって確認された情報（コンテンツの利用条件や不正利用した場合の処置や電子透かしの抽出法など）に対するユーザの同意書ファイルであり、1 3 0 7 は店頭などで売られている暗号化されたデジタルコンテンツが入った CD-ROM などの記憶媒体である。

【 0 0 9 4 】

次に、図 1 4 のフローチャートを用いて本システムの動作について説明する。

【 0 0 9 5 】

ユーザ 1 3 0 2 は店頭などから CD-ROM 1 3 0 7 を購入する（ステップ S 1 4 0 1）。ユーザ 1 3 0 2 は CD-ROM 1 3 0 7 に含まれる説明／抽出ソフト 1 3 0 5 を立ち上げ、コンテンツの利用条件や不正利用した場合の処置及び電子透かしの抽出法に関する説明を受ける（ステップ S 1 4 0 2）。CD-ROM 1 3 0 7 にはサンプルコンテンツがあり練習できるようになっていてもよい。次に、ユーザ 1 3 0 2 は説明／抽出ソフト 1 3 0 5 の説明を理解し同意書 1 3 0 6 を作成しネットワーク 1 3 0 1 を用いて CD-ROM 番号とともに販売局 1 3 0 3 に送信する（ステップ S 1 4 0 3）。この同意書 1 3 0 6 には前述のデジタル署名が添付されていることが望ましい。ユーザ 1 3 0 2 の端末がネットワークに接続されていない場合、ユーザ 1 3 0 2 は電話や FAX、郵便など他の手段によって印刷された同意書及び CD-ROM 番号を販売局 1 3 0 3 に送付する。販

売局 1 3 0 3 は受け取った同意書 1 3 0 6 を確認して保存する（ステップ S 1 4 0 4）。販売局はユーザ 1 3 0 2 が購入を申請したコンテンツ 1 3 0 4 に対する暗号化を復号するための復号鍵をネットワークまたは指定された手段でユーザ 1 3 0 2 に送信する（ステップ S 1 4 0 5）。ユーザは送られてきた復号鍵でコンテンツ 1 3 0 4 を復号し、説明／抽出ソフト 1 3 0 5 を用いて電子透かしの抽出確認をする（ステップ S 1 4 0 6）。最後に、販売局 1 3 0 3 は同意書とともに送られた C D - R O M 番号やユーザ 1 3 0 2 が購入したコンテンツの I D をユーザ情報と一緒にデータベース化して管理する（ステップ S 1 4 0 7）。

#### 【 0 0 9 6 】

同意書作成及び C D - R O M 番号送付は説明／抽出ソフト 1 3 0 5 を実行した際、ユーザからのいくつかの入力以外は自動的に行われるようになっていてもよい。さらに、暗号化コンテンツの復号や電子透かし抽出も説明／抽出ソフト 1 3 0 5 によってユーザからのいくつかの入力以外は自動的に行われてもよい。

#### 【 0 0 9 7 】

本実施の形態では C D - R O M 番号及び／またはコンテンツ I D を各コンテンツに埋め込み、かつ販売局 1 3 0 3 がその C D - R O M 番号やコンテンツ I D とユーザ情報を一緒にデータベース管理することによって不正ユーザを特定できる。つまり、不正なデジタルコンテンツが見つかった場合、そのコンテンツに C D - R O M 番号及び／またはコンテンツ I D が埋め込まれていれば、その I D からデータベースを検索しそのコンテンツを購入したユーザを特定できる。

#### 【 0 0 9 8 】

なお、本実施の形態においても同意書の作成、送付の手順は省略することができる。

#### 【 0 0 9 9 】

##### （他の実施の形態）

本発明の第 4、第 5 の実施の形態では説明／抽出ソフトを各ユーザに配布する例を示したが、該ソフトを配布せずホームページへのリンク情報を示すだけにすることもできる。この場合、そのホームページにはデジタルコンテンツの利用条件の説明や電子透かし抽出ソフトの説明があり、そこから電子透かし抽出ソフ

トをダウンロードすることができればよい。

【0100】

さらに、ホームページ上に公開された電子透かし抽出ソフトはデジタルコンテンツを購入するユーザだけでなく、ネットワークに接続できるすべてのユーザによってダウンロードできる。よって、多くのユーザが電子透かし抽出ソフトをダウンロードし、自分がアクセスする他のユーザ端末のデジタルコンテンツをそのソフトによって検査し、その結果を前述のホームページに示されている連絡先などに端末の通信機能などを用いて連結すればデジタルコンテンツの検査システムが構築できるという利点もある。

【0101】

なお、本発明は、複数の機器（例えばホストコンピュータ、インタフェイス機器、リーダ、プリンタなど）から構成されるシステムに適用しても、一つの機器からなる装置（例えば、複写機、ファクシミリ装置など）に適用してもよい。

【0102】

また、本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体（または記録媒体）を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはCPUやMPU）が記憶媒体に格納されたプログラムコードを読み出し実行することによっても、達成されることは言うまでもない。この場合、記憶媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているオペレーティングシステム（OS）などが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【0103】

さらに、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張カードやコンピュータに接続された機能拡張ユニットに備わるメ

モリに書込まれた後、そのプログラムコードの指示に基づき、その機能拡張カードや機能拡張ユニットに備わるCPUなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【0104】

本発明を上記記憶媒体に適用する場合、その記憶媒体には、先に説明したフローチャートに対応するプログラムコードが格納されることになる。

【0105】

【発明の効果】

本発明によれば、効率的に且つ確実に著作権を保護することのできる検査方法及び検査システムを提供することができる。

【図面の簡単な説明】

【図1】

本発明の第1の実施の形態におけるシステムの概要を説明する図である。

【図2】

第1の実施の形態におけるエージェントの概要を説明する図である。

【図3】

第1の実施の形態におけるシステムの処理手順の概要を説明する図である。

【図4】

第2の実施の形態におけるシステムの概要を説明する図である。

【図5】

第2の実施の形態におけるシステムの概要を説明する図である。

【図6】

第3の実施の形態におけるシステムの概要を説明する図である。

【図7】

第3の実施の形態におけるシステムの処理手順の概要を説明する図である。

【図8】

端末の内部構成を説明する概略図である。

【図9】

第 3 の実施の形態におけるシステムの処理手順の概要を説明する図である。

【図 1 0】

第 3 の実施の形態におけるシステムの処理手順の概要を説明する図である。

【図 1 1】

第 4 の実施の形態におけるシステムの概要を説明する図である。

【図 1 2】

第 4 の実施の形態におけるシステムの処理手順を説明する図である。

【図 1 3】

第 5 の実施の形態におけるシステムの概要を説明する図である。

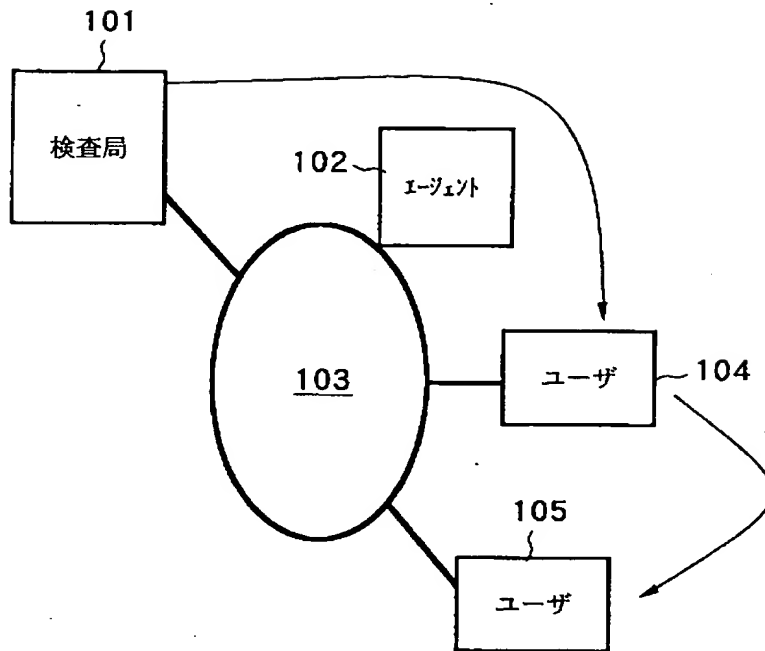
【図 1 4】

第 5 の実施の形態におけるシステムの処理手順を説明する図である。

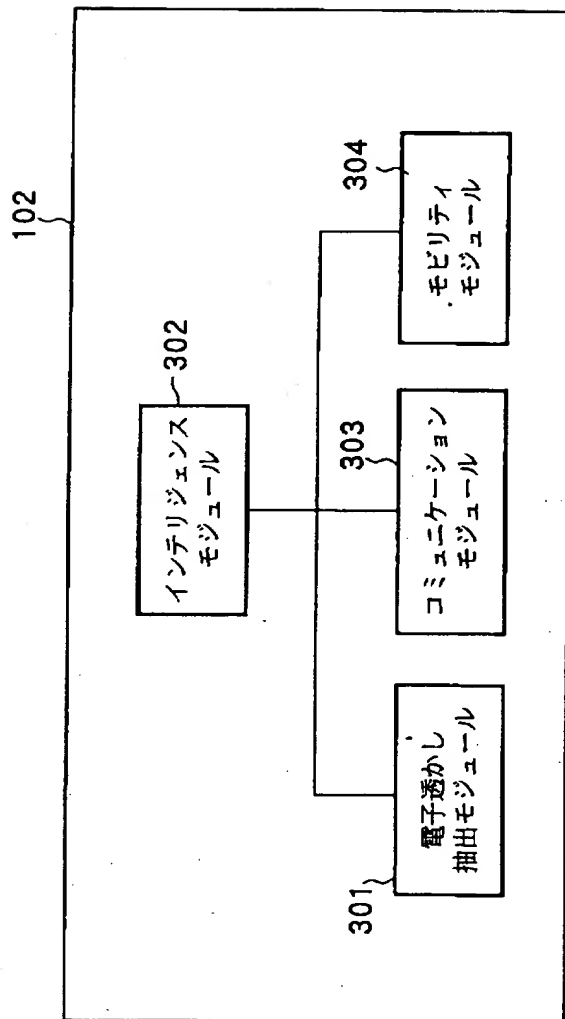


【書類名】 図面

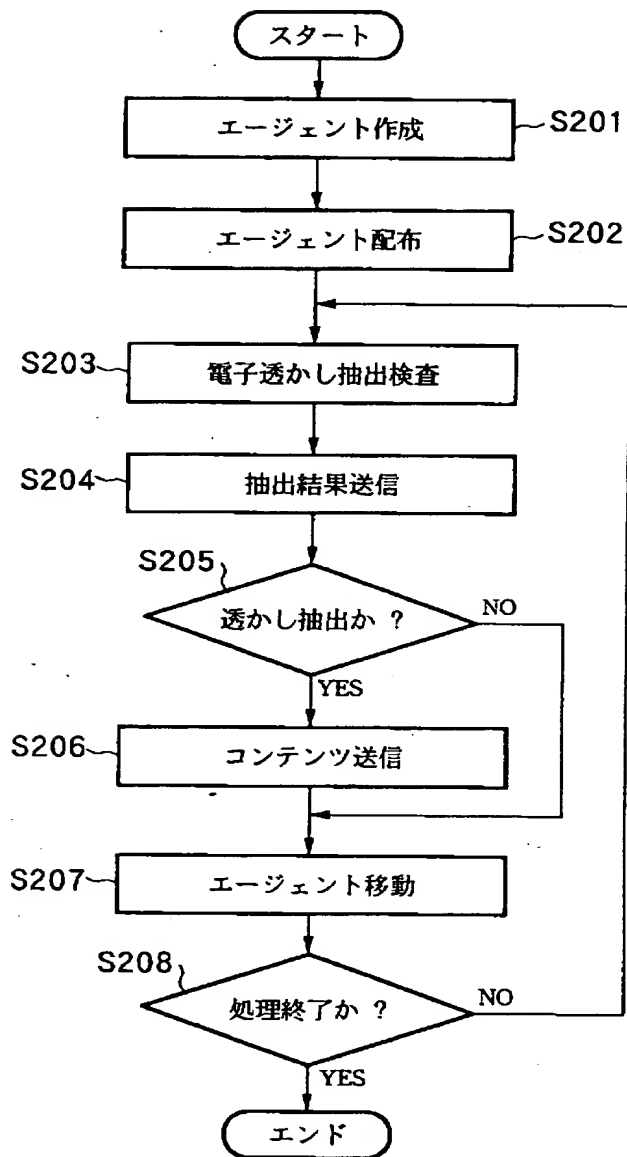
【図 1】



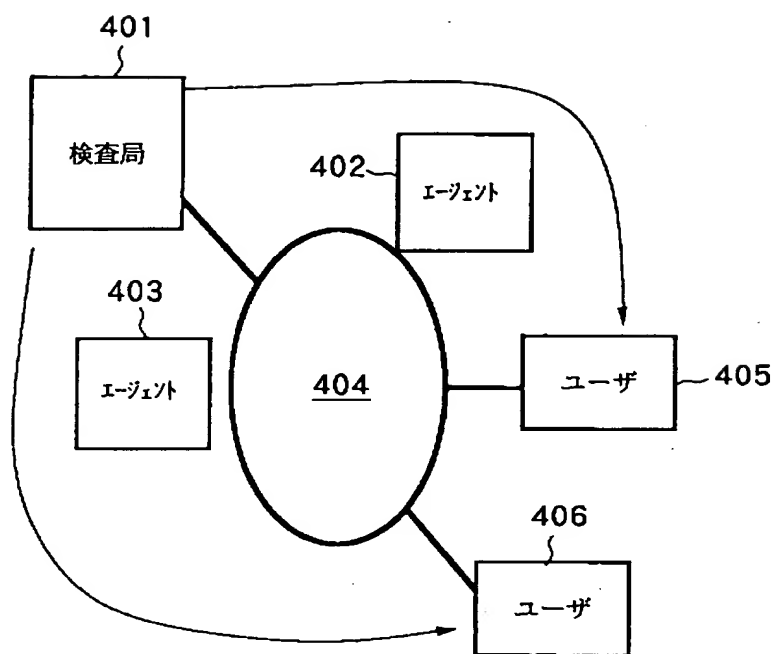
【図 2】



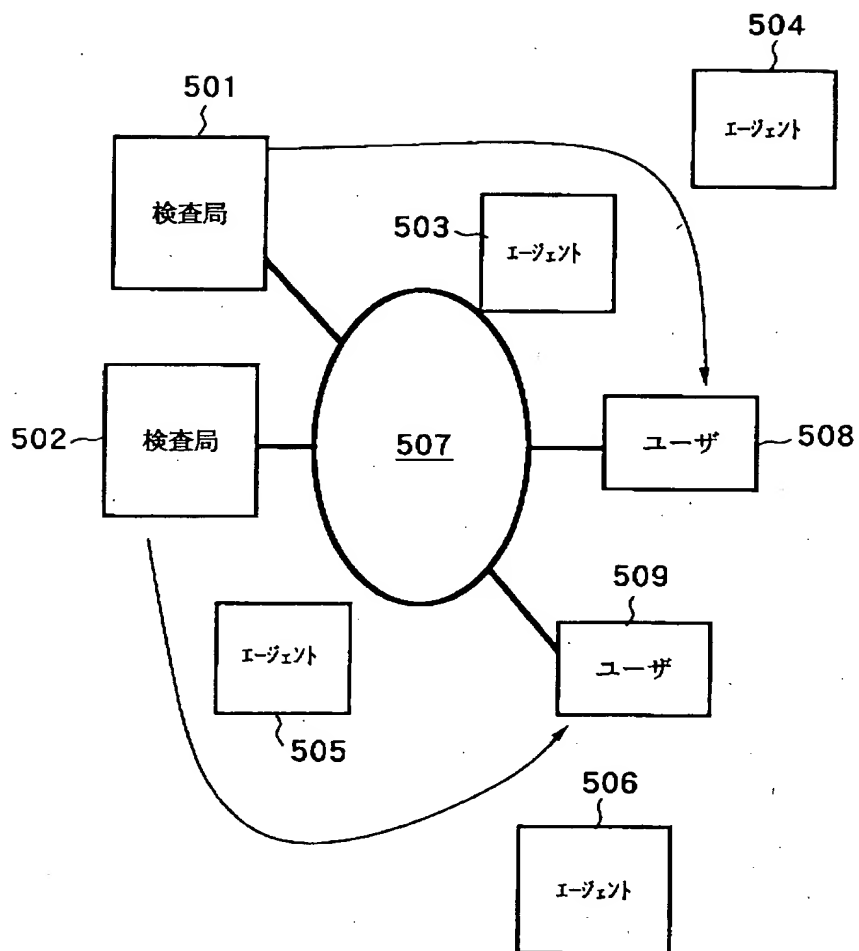
【図 3】



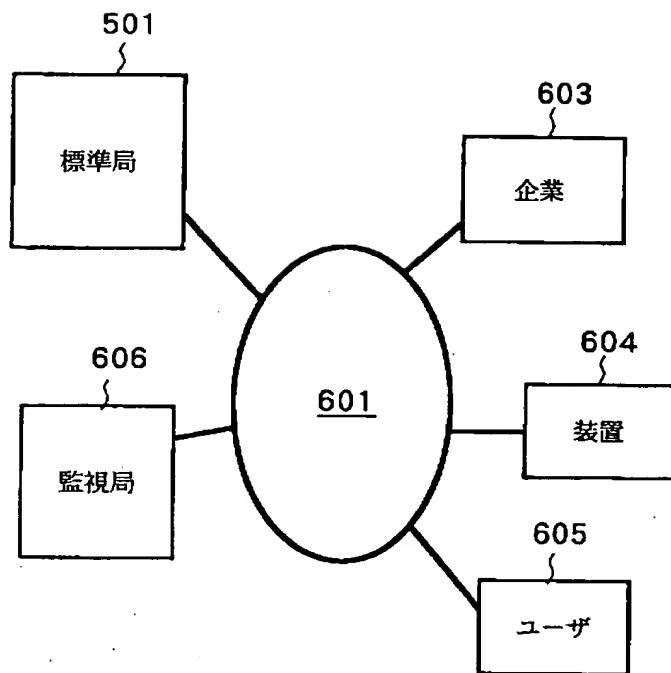
【図 4】



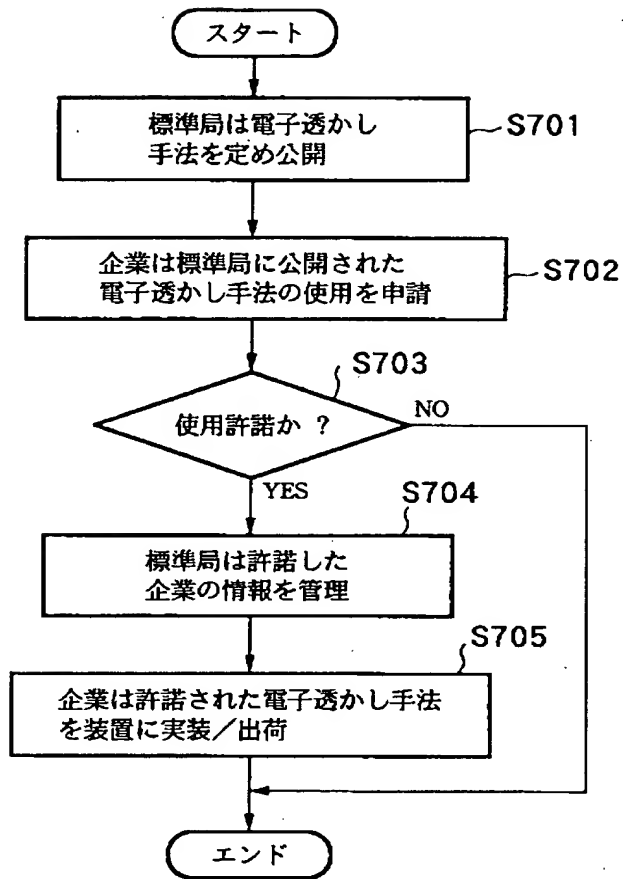
【図 5】



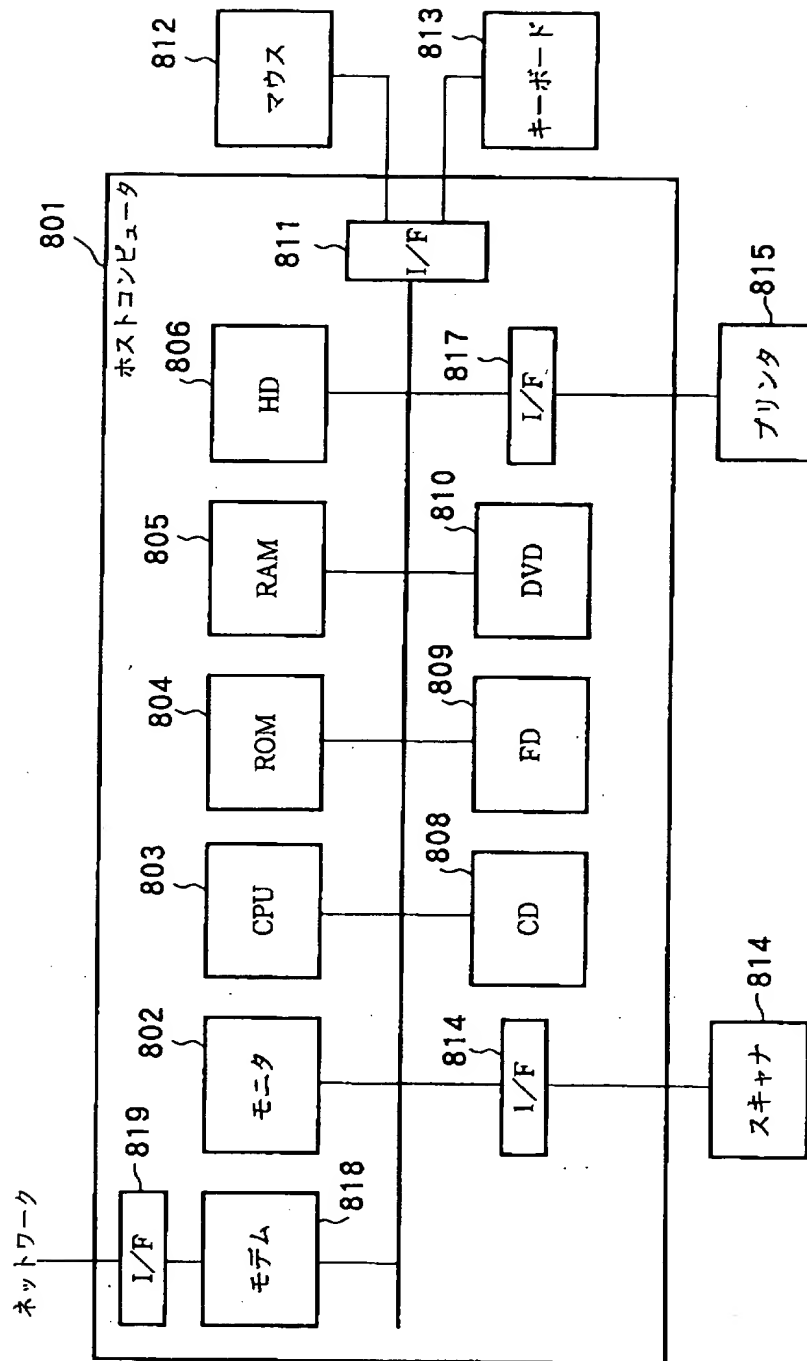
【図 6】



【図 7】

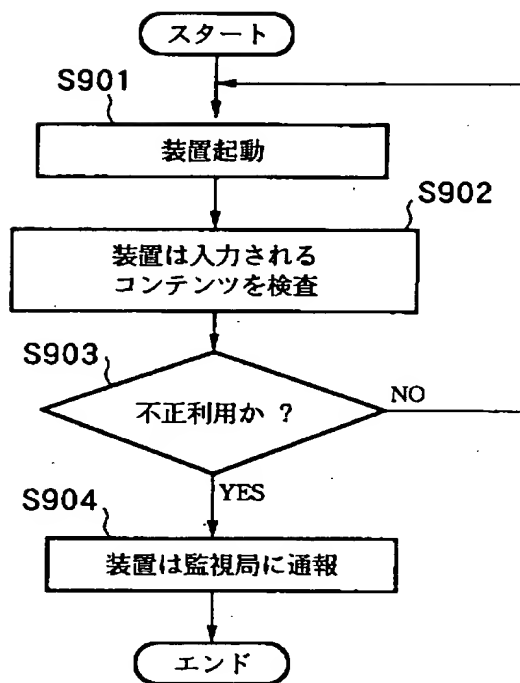


【図 8】

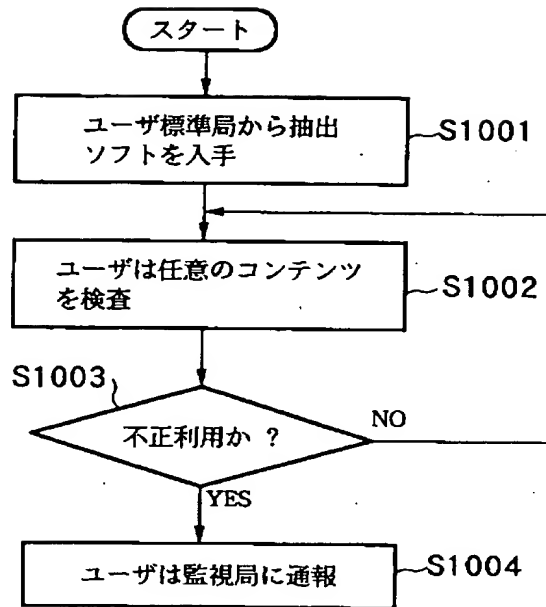




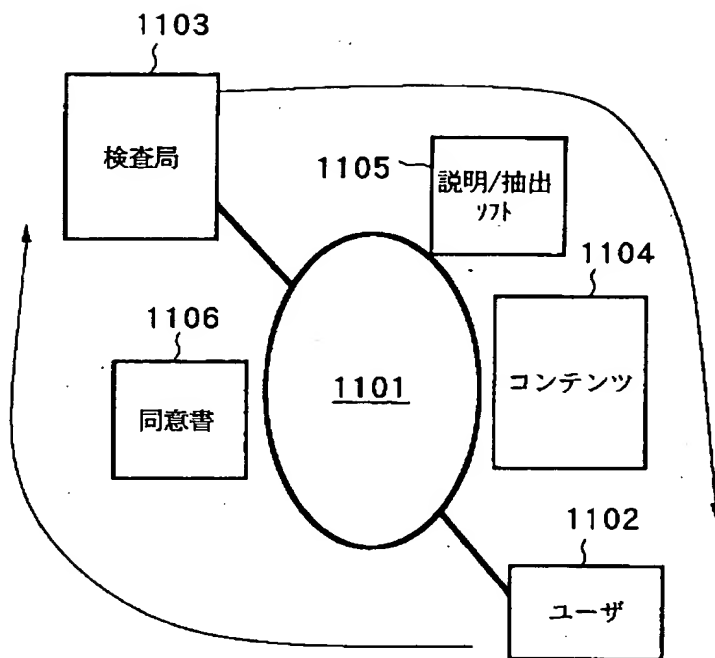
【図 9】



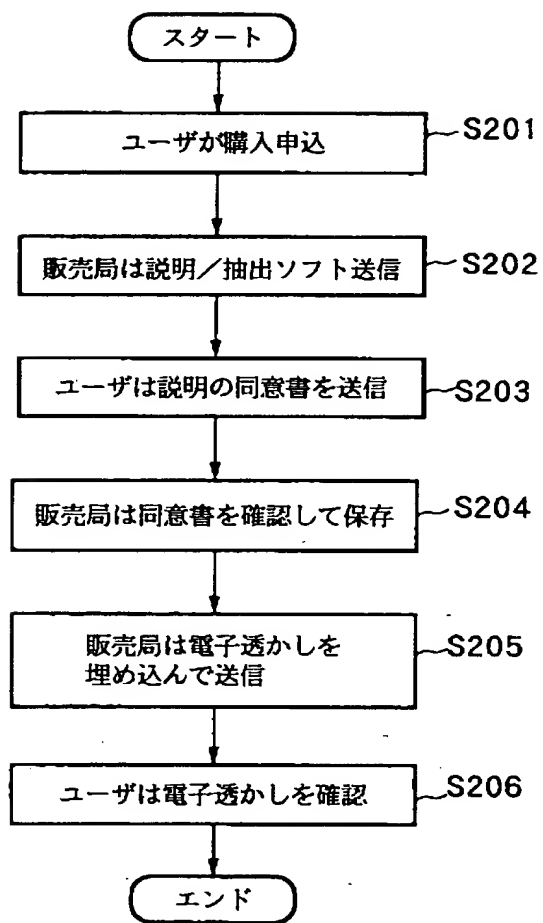
【図 1 0】



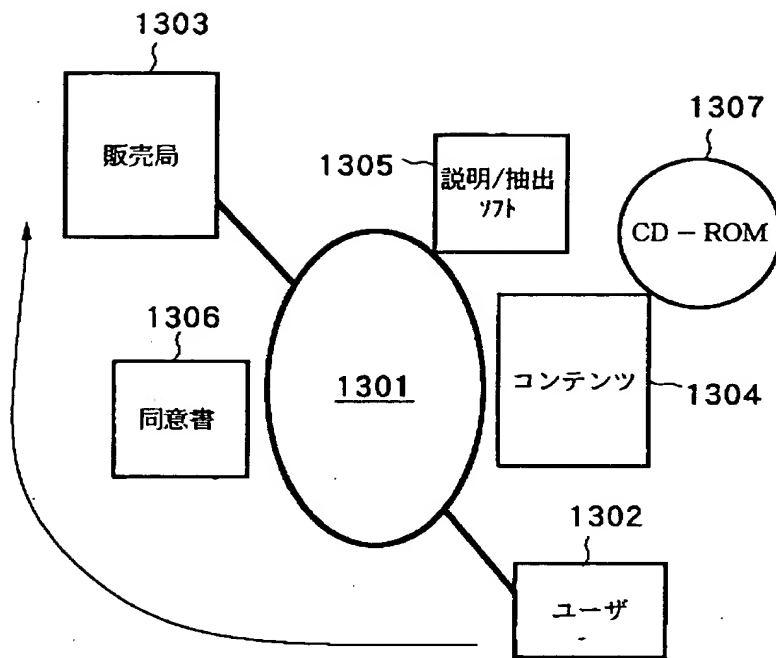
【図 1 1】



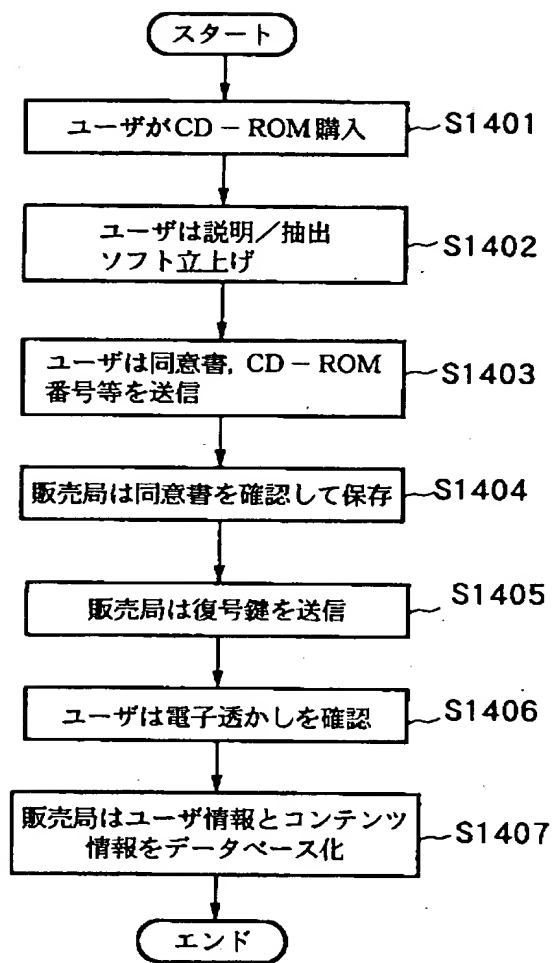
【図 1 2】



【図 1 3】



【図 1 4】



【書類名】 要約書

【要約】

【課題】 効率的に且つ確実に著作権を保護することのできる検査方法及び検査システムを提供すること。

【解決手段】 ネットワーク 1 0 3 を構成する端末 1 0 4 に格納された情報を検査する検査方法であって、

端末 1 0 4 間を移動し、情報に電子透かしが埋め込まれているか否かを判定するロボットエージェント 1 0 2 を利用することを特徴とする。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000001007]

1. 変更年月日 1990年 8月30日  
[変更理由] 新規登録  
住 所 東京都大田区下丸子3丁目30番2号  
氏 名 キヤノン株式会社